

Quản trị phân quyền

MÃ HP: 123041 - HỆ ĐIỀU HÀNH LINUX

Mục tiêu

Tìm hiểu về chủ sở hữu, nhóm sở hữu quyền truy cập trên HĐH Linux

Tìm hiểu các lệnh liên quan đến chủ sở hữu, nhóm sở hữu quyền truy cập trên HĐH Linux

Tìm hiểu SUID, SGID, Sticky Bit, Access Control List

Giới thiệu

Trên Linux, quyền được sử dụng để xác định người dùng và nhóm nào có quyền truy cập vào tập tin và thư mục.

Kiểm soát quyền và quyền truy cập vào các tập tin và ứng dụng của hệ thống là rất quan trọng đối với bảo mật trên máy chủ Linux.

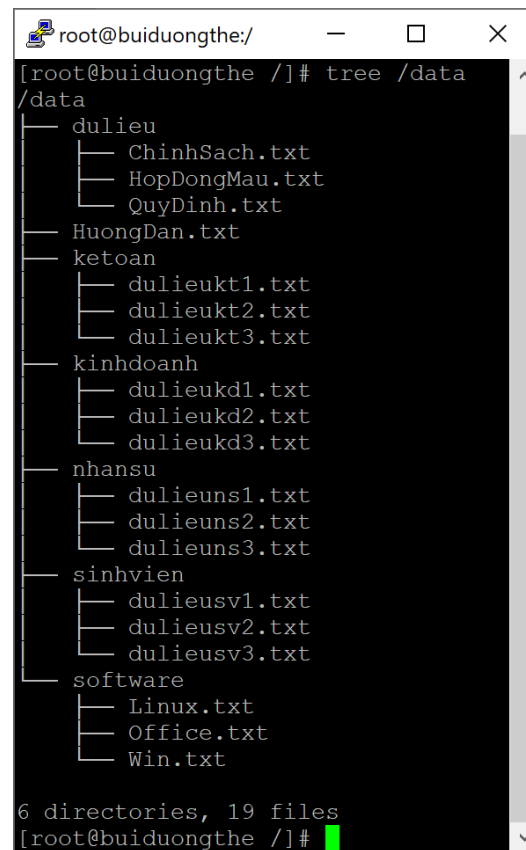
Do đó, điều quan trọng là phải hiểu cách hoạt động của các quyền và cách thay đổi các quyền.

1. Khởi tạo thư mục

```
# mkdir -p  
/data/{ketoan,kinhdoanh,nhansu,sinhvien,dulieu,software}
```

```
# cd /data/ketoan/
```

```
# touch dulieukt1.txt dulieukt2.txt  
dulieukt3.txt
```



```
root@buiduongthe:/  
[root@buiduongthe /]# tree /data  
/data  
├── dulieu  
│   ├── ChinhSach.txt  
│   ├── HopDongMau.txt  
│   └── QuyDinh.txt  
├── HuongDan.txt  
├── ketoan  
│   ├── dulieukt1.txt  
│   ├── dulieukt2.txt  
│   └── dulieukt3.txt  
├── kinhdoanh  
│   ├── dulieukd1.txt  
│   ├── dulieukd2.txt  
│   └── dulieukd3.txt  
├── nhansu  
│   ├── dulieuns1.txt  
│   ├── dulieuns2.txt  
│   └── dulieuns3.txt  
├── sinhvien  
│   ├── dulieusv1.txt  
│   ├── dulieusv2.txt  
│   └── dulieusv3.txt  
└── software  
    ├── Linux.txt  
    ├── Office.txt  
    └── Win.txt  
  
6 directories, 19 files  
[root@buiduongthe /]#
```

2. Khảo sát thư mục

ll -l /data/

stat /data/

- **Unix file type**
- **Permissions**
- Number of hard links
- **Owner**
- **Group**
- Size
- Date and time
- Name

```
buiduongthe@buiduongthe:/home/buiduongthe
File Edit View Search Terminal Help
[root@buiduongthe buiduongthe]# ll -l /data
total 0
drwxr-xr-t. 2 root root 68 Oct 9 09:43 dulieu
-rw-r--r--. 1 root root 0 Oct 9 09:47 HuongDan.txt
drwxrwx--T. 2 root root 69 Oct 9 09:40 ketoan
drwxrwsr-t. 3 root root 112 Oct 9 16:32 kinhdoanh
drwxrwxr-t. 2 root root 163 Oct 9 16:58 nhansu
drwxr-xr-x. 2 root root 69 Oct 9 09:42 sinhvien
drwxr-xr-x. 2 root root 83 Oct 9 16:11 software
[root@buiduongthe buiduongthe]#
```

```
root@buiduongthe:/
[root@buiduongthe /]# ll -l /data/
total 0
drwxr-xr-x. 2 root root 68 Oct 9 09:43 dulieu
-rw-r--r--. 1 root root 0 Oct 9 09:47 HuongDan.txt
drwxr-xr-x. 2 root root 69 Oct 9 09:40 ketoan
drwxr-xr-x. 2 root root 69 Oct 9 09:42 kinhdoanh
drwxr-xr-x. 2 root root 69 Oct 9 09:42 nhansu
drwxr-xr-x. 2 root root 69 Oct 9 09:42 sinhvien
drwxr-xr-x. 2 root root 56 Oct 9 09:44 software
[root@buiduongthe /]#
```

2. Khảo sát thư mục

ll -l /data/

Unix file type	Description
-	File
d	Directory
l	Link
C	Character devices
B	Block devices
s	Socket
p	Named pipe

ll -l /dev

```
root@buiduongthe:/  
[root@buiduongthe /]# ll -l /data/  
total 0  
drwxr-xr-x. 2 root root 68 Oct  9 09:43 dulieu  
-rw-r--r--. 1 root root  0 Oct  9 09:47 HuongDan.txt  
drwxr-xr-x. 2 root root 69 Oct  9 09:40 ketoan  
drwxr-xr-x. 2 root root 69 Oct  9 09:42 kinhdoanh  
drwxr-xr-x. 2 root root 69 Oct  9 09:42 nhansu  
drwxr-xr-x. 2 root root 69 Oct  9 09:42 sinhvien  
drwxr-xr-x. 2 root root 56 Oct  9 09:44 software  
[root@buiduongthe /]#
```

ll -l /dev/ | grep -w 'zero\|shm\|rtc'

ll -l /run/ | grep -e 'mcev*\|dmel*'

3. Khảo sát phân quyền

ll -l /data/

Value	Character	Description
0	-	No Permission
4	R	Read only
2	W	Write only
1	X	Execute

```
root@buiduongthe:/  
[root@buiduongthe /]# ll -l /data/  
total 0  
drwxr-xr-x. 2 root root 68 Oct 9 09:43 dulieu  
-rw-r--r--. 1 root root 0 Oct 9 09:47 HuongDan.txt  
drwxr-xr-x. 2 root root 69 Oct 9 09:40 ketoan  
drwxr-xr-x. 2 root root 69 Oct 9 09:42 kinhdoanh  
drwxr-xr-x. 2 root root 69 Oct 9 09:42 nhansu  
drwxr-xr-x. 2 root root 69 Oct 9 09:42 sinhvien  
drwxr-xr-x. 2 root root 56 Oct 9 09:44 software  
[root@buiduongthe /]#
```

3. Khảo sát phân quyền

Onwer	Group	Other
R W X	R W X	R W X

Character	Description
-	No Permission
R	Read only
W	Write only
X	Execute

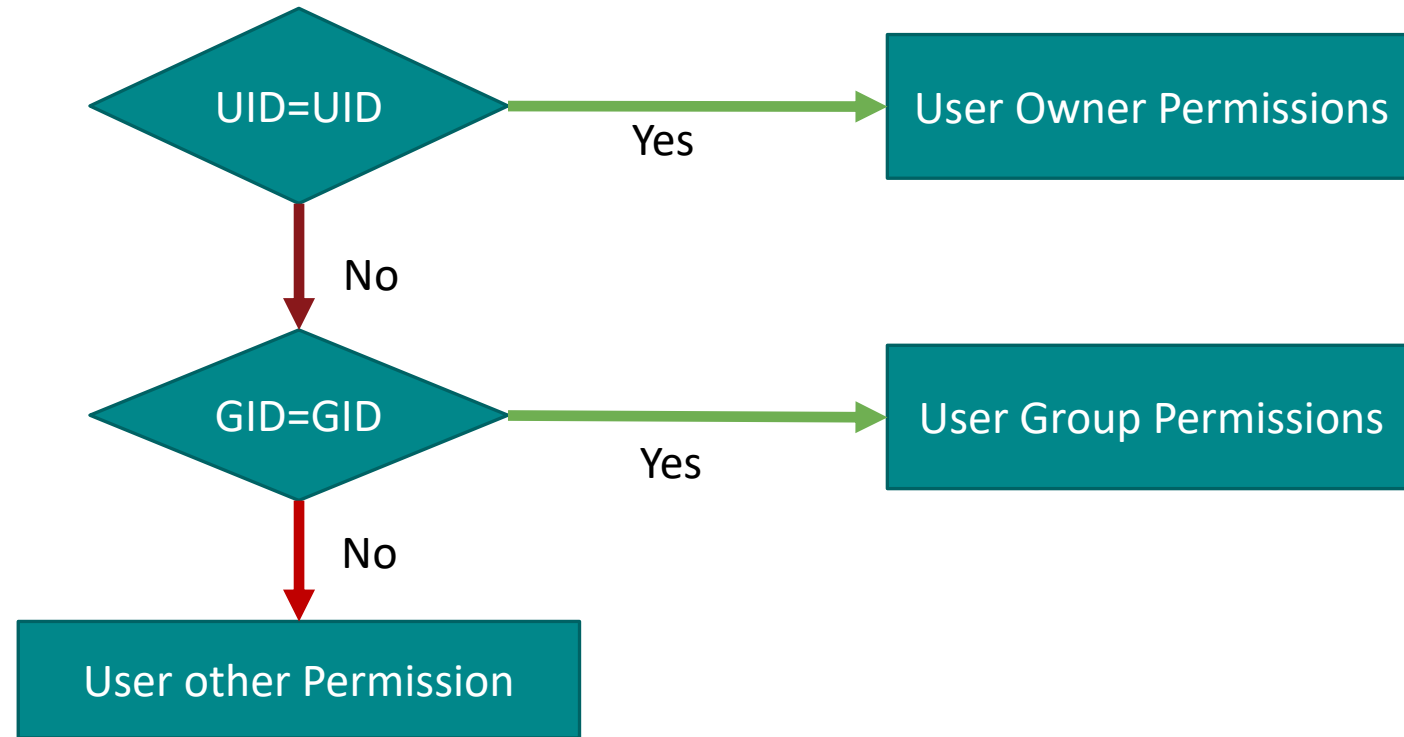
Character	Description
-	No Permission
R	Read only
W	Write only
X	Execute

Character	Description
-	No Permission
R	Read only
W	Write only
X	Execute

4. Bảng phân quyền

Octal	Value Permission	Sets Binary	Octal Number	Permissions
7	rwX	111 (4+2+1)	600	rw-----
6	rw-	110 (4+2+0)	644	rw-r--r--
5	r-X	101 (4+0+1)	664	rw-rw-r--
4	r--	100 (4+0+0)	666	rw-rw-rw-
3	-wX	011 (0+2+1)	755	rwXr-Xr-X
2	-w-	010 (0+2+0)	777	rwXrwXrwX
1	--X	001 (0+0+1)		
0	---	000 (0+0+0)		

5. Xác định quyền truy cập



6. Thay đổi quyền sở hữu chown

cd /data

ll -l

chown --help

chown nv1 dulieu

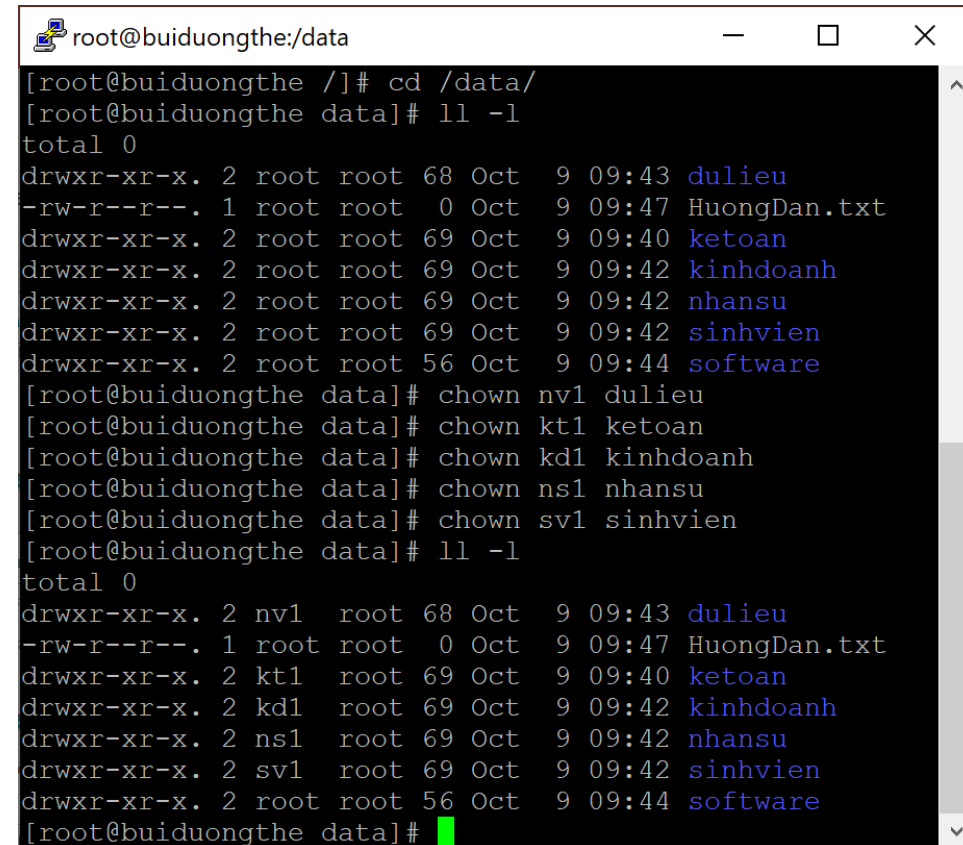
chown kt1 ketoan

chown kd1 kinhdoanh

chown ns1 nhansu

chown sv1 sinhvien

ll -l



```
root@buiduongthe:/data
[root@buiduongthe /]# cd /data/
[root@buiduongthe data]# ll -l
total 0
drwxr-xr-x. 2 root root 68 Oct  9 09:43 dulieu
-rw-r--r--. 1 root root  0 Oct  9 09:47 HuongDan.txt
drwxr-xr-x. 2 root root 69 Oct  9 09:40 ketoan
drwxr-xr-x. 2 root root 69 Oct  9 09:42 kinhdoanh
drwxr-xr-x. 2 root root 69 Oct  9 09:42 nhansu
drwxr-xr-x. 2 root root 69 Oct  9 09:42 sinhvien
drwxr-xr-x. 2 root root 56 Oct  9 09:44 software
[root@buiduongthe data]# chown nv1 dulieu
[root@buiduongthe data]# chown kt1 ketoan
[root@buiduongthe data]# chown kd1 kinhdoanh
[root@buiduongthe data]# chown ns1 nhansu
[root@buiduongthe data]# chown sv1 sinhvien
[root@buiduongthe data]# ll -l
total 0
drwxr-xr-x. 2 nv1  root 68 Oct  9 09:43 dulieu
-rw-r--r--. 1 root root  0 Oct  9 09:47 HuongDan.txt
drwxr-xr-x. 2 kt1  root 69 Oct  9 09:40 ketoan
drwxr-xr-x. 2 kd1  root 69 Oct  9 09:42 kinhdoanh
drwxr-xr-x. 2 ns1  root 69 Oct  9 09:42 nhansu
drwxr-xr-x. 2 sv1  root 69 Oct  9 09:42 sinhvien
drwxr-xr-x. 2 root root 56 Oct  9 09:44 software
[root@buiduongthe data]#
```

7. Thay đổi nhóm sở hữu chgrp

```
# cd /data
```

```
# ll -l
```

```
# chgrp --help
```

```
# chgrp users dulieu
```

```
# chgrp users software
```

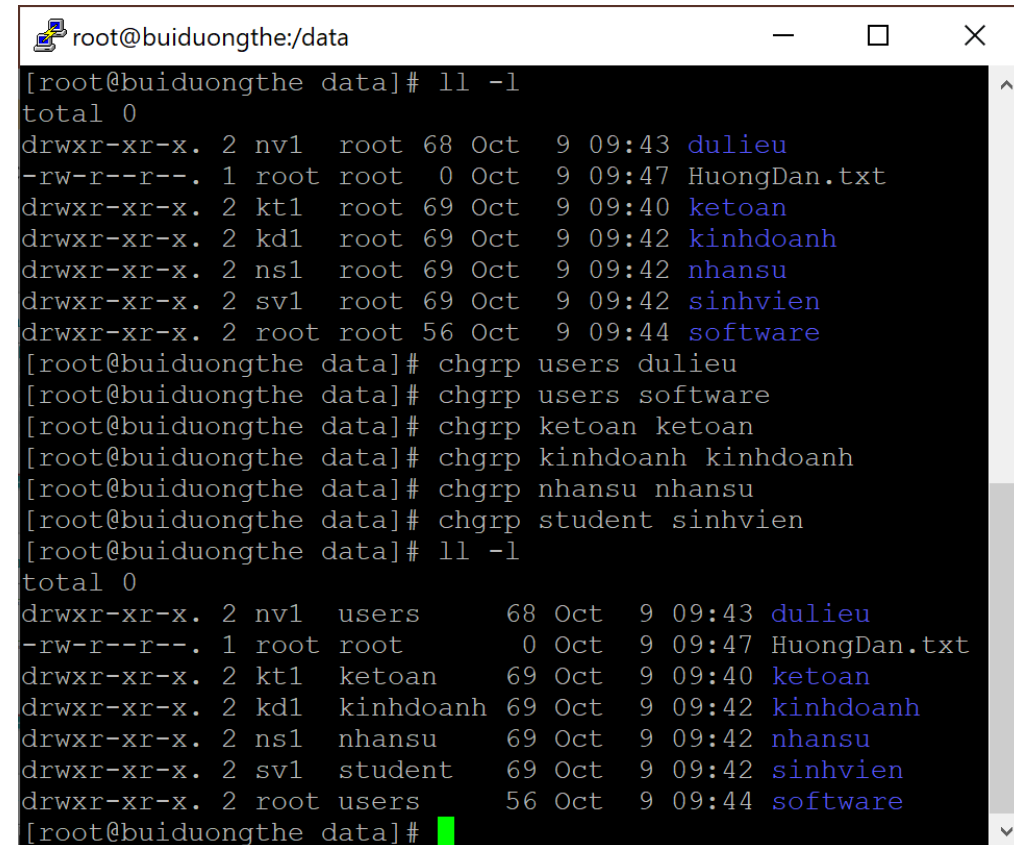
```
# chgrp ketoan ketoan
```

```
# chgrp kinhdoanh kinhdoanh
```

```
# chgrp nhansu nhansu
```

```
# chgrp student sinhvien
```

```
# ll -l
```



```
root@buiduongthe:/data
[root@buiduongthe data]# ll -l
total 0
drwxr-xr-x. 2 nv1 root 68 Oct 9 09:43 dulieu
-rw-r--r--. 1 root root 0 Oct 9 09:47 HuongDan.txt
drwxr-xr-x. 2 kt1 root 69 Oct 9 09:40 ketoan
drwxr-xr-x. 2 kd1 root 69 Oct 9 09:42 kinhdoanh
drwxr-xr-x. 2 ns1 root 69 Oct 9 09:42 nhansu
drwxr-xr-x. 2 sv1 root 69 Oct 9 09:42 sinhvien
drwxr-xr-x. 2 root root 56 Oct 9 09:44 software
[root@buiduongthe data]# chgrp users dulieu
[root@buiduongthe data]# chgrp users software
[root@buiduongthe data]# chgrp ketoan ketoan
[root@buiduongthe data]# chgrp kinhdoanh kinhdoanh
[root@buiduongthe data]# chgrp nhansu nhansu
[root@buiduongthe data]# chgrp student sinhvien
[root@buiduongthe data]# ll -l
total 0
drwxr-xr-x. 2 nv1 users 68 Oct 9 09:43 dulieu
-rw-r--r--. 1 root root 0 Oct 9 09:47 HuongDan.txt
drwxr-xr-x. 2 kt1 ketoan 69 Oct 9 09:40 ketoan
drwxr-xr-x. 2 kd1 kinhdoanh 69 Oct 9 09:42 kinhdoanh
drwxr-xr-x. 2 ns1 nhansu 69 Oct 9 09:42 nhansu
drwxr-xr-x. 2 sv1 student 69 Oct 9 09:42 sinhvien
drwxr-xr-x. 2 root users 56 Oct 9 09:44 software
[root@buiduongthe data]#
```

8. Thay đổi quyền truy cập chmod

```
chmod symbolic_mode filename
```

Who / Option / Permissions

Who	Option	Permmision
u Owner (user) Permissions	+ Add Permissions	r Read
g Group Permissions	- Remove Permissions	w Write
o Other Permissions	= Assign Permissions Absolutely	x Execute
a All Permissions (Owner, Group, Other)		

8. Thay đổi quyền truy cập chmod

Thực hiện cấp thêm quyền Write cho nhóm kế toán và hủy quyền của các other user

```
# ll -l | grep ketoan
```

```
# chmod g+w,o-xr ketoan
```

Đăng nhập tài khoản kd1 và kt1 để truy cập vào thư mục của ketoan và kiểm tra các quyền R,W,X

```
root@buiduongthe:/data
[root@buiduongthe data]# ll -l | grep ketoan
drwxr-xr-x. 2 kt1 ketoan 69 Oct 9 09:40 ketoan
[root@buiduongthe data]# chmod g+w,o-xr ketoan
[root@buiduongthe data]# ll -l | grep ketoan
drwxrwx---. 2 kt1 ketoan 69 Oct 9 09:40 ketoan
[root@buiduongthe data]#
```

```
kd1@buiduongthe:~
Using username "kd1".
kd1@192.168.1.17's password:
Last login: Sun Oct 9 14:46:03 2022
[kd1@buiduongthe ~]$ cd /data/ketoan/
-bash: cd: /data/ketoan/: Permission denied
[kd1@buiduongthe ~]$
```

```
kt1@buiduongthe:~
[kt1@buiduongthe ~]$ cat /data/ketoan/dulieukt1.txt
Du lieu ke toan
[kt1@buiduongthe ~]$
```

9. Sửa quyền truy cập mặc định

Thư mục có quyền mặc định là **777**

Tập tin có quyền mặc định là **666**

Với **umask = 022** thì:

Thư mục: $777 - 022 = 755$

Tập tin: $666 - 022 = 644$

umask

mkdir /data/umask

touch /data/umask.txt

ll -l /data/ | **grep** umask

```
root@buiduongthe:~  
[root@buiduongthe ~]# umask  
0022  
[root@buiduongthe ~]#
```

```
root@buiduongthe:~  
[root@buiduongthe ~]# mkdir /data/umask  
[root@buiduongthe ~]# touch /data/umask.txt  
[root@buiduongthe ~]# ll -l /data/ | grep umask  
drwxr-xr-x. 2 root root    6 Oct  9 15:37 umask  
-rw-r--r--. 1 root root    0 Oct  9 15:37 umask.txt
```

9. Sửa quyền truy cập mặc định

Thay đổi **umask**

umask 007

Với **umask = 007** thì:

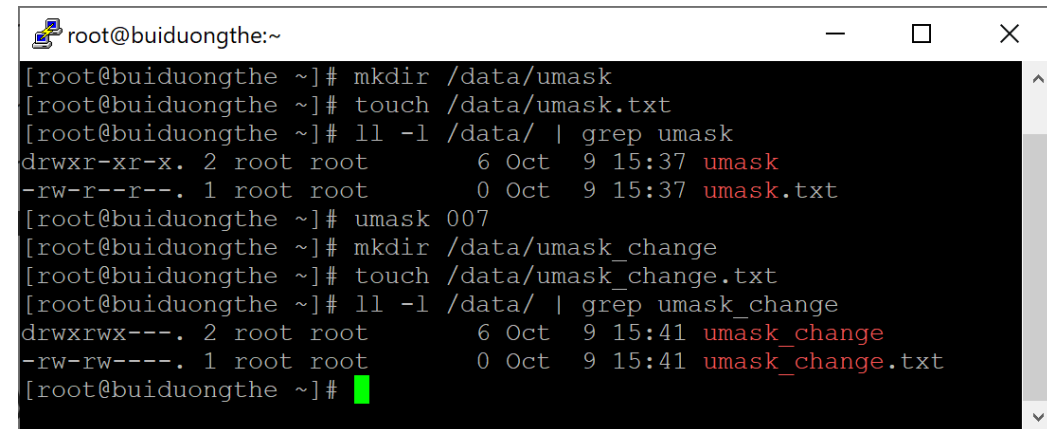
Thư mục: $777 - 007 = 770$

Tập tin: $666 - 007 = 660$

mkdir /data/umask_change

touch /data/umask_change.txt

ll -l /data/ | grep umask_change



```
root@buiduongthe:~  
[root@buiduongthe ~]# mkdir /data/umask  
[root@buiduongthe ~]# touch /data/umask.txt  
[root@buiduongthe ~]# ll -l /data/ | grep umask  
drwxr-xr-x. 2 root root    6 Oct  9 15:37 umask  
-rw-r--r--. 1 root root    0 Oct  9 15:37 umask.txt  
[root@buiduongthe ~]# umask 007  
[root@buiduongthe ~]# mkdir /data/umask_change  
[root@buiduongthe ~]# touch /data/umask_change.txt  
[root@buiduongthe ~]# ll -l /data/ | grep umask_change  
drwxrwx---. 2 root root    6 Oct  9 15:41 umask_change  
-rw-rw----. 1 root root    0 Oct  9 15:41 umask_change.txt  
[root@buiduongthe ~]#
```


9. Sửa quyền truy cập mặc định

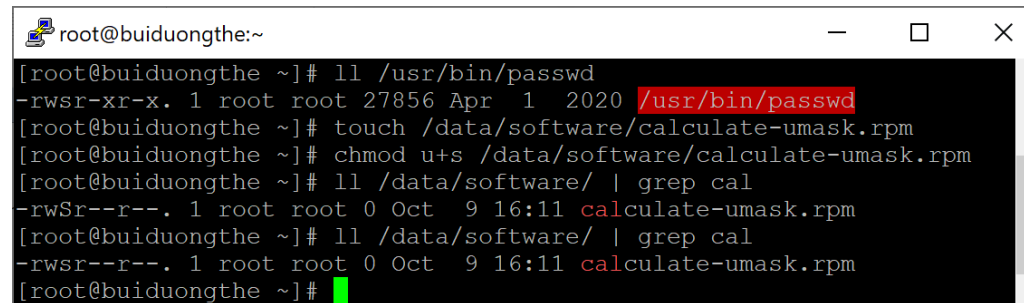
Umark thường dùng

Set umask	User	Group	Other
000	All	All	All
007	All	All	None
026	All	Read/Execute	None

Set umask	Security level	Permission
022	Permissive	755
026	Moderate	751
027	Moderate	750
077	Severe	700

10. SUID

SUID hoặc Set UID, user ID: Nếu bit SUID được thiết lập cho ứng dụng hoặc tập tin thực thi thì một tài khoản nào đó bất kỳ không phải là chủ sở hữu cũng có thể sử dụng để thực thi.

A terminal window titled 'root@buiduongthe:~' with standard window controls. It shows a series of commands and their outputs. The command 'll /usr/bin/passwd' shows the file permissions '-rwsr-xr-x'. The command 'touch /data/software/calculate-umask.rpm' is executed. The command 'chmod u+s /data/software/calculate-umask.rpm' is executed. The command 'll /data/software/ | grep cal' is executed twice, showing the file permissions '-rwsr--r--' for 'calculate-umask.rpm'.

```
root@buiduongthe:~  
[root@buiduongthe ~]# ll /usr/bin/passwd  
-rwsr-xr-x. 1 root root 27856 Apr  1 2020 /usr/bin/passwd  
[root@buiduongthe ~]# touch /data/software/calculate-umask.rpm  
[root@buiduongthe ~]# chmod u+s /data/software/calculate-umask.rpm  
[root@buiduongthe ~]# ll /data/software/ | grep cal  
-rwsr--r--. 1 root root 0 Oct  9 16:11 calculate-umask.rpm  
[root@buiduongthe ~]# ll /data/software/ | grep cal  
-rwsr--r--. 1 root root 0 Oct  9 16:11 calculate-umask.rpm  
[root@buiduongthe ~]#
```

10. SUID

touch /data/software/calculate-umask.rpm

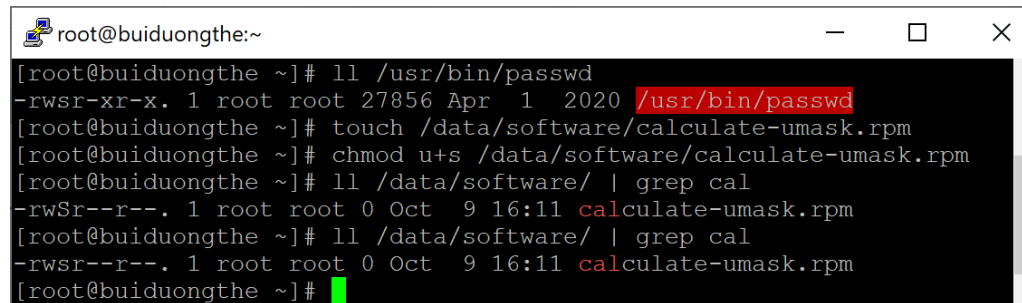
chmod u+s /data/software/calculate-umask.rpm

Hoặc

chmod 4644 /data/software/calculate-umask.rpm

Nếu tập tin chưa có quyền thực thi thì SUID là chữ **S**, ngược lại là chữ **s**

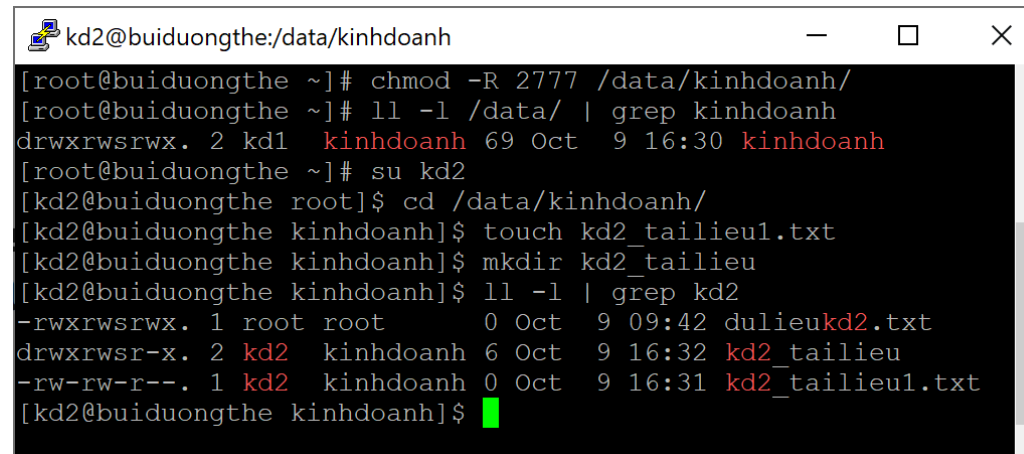
chmod 4744 /data/software/calculate-umask.rpm

A terminal window titled 'root@buiduongthe:~' showing a series of commands and their outputs. The commands include 'll /usr/bin/passwd', 'touch /data/software/calculate-umask.rpm', 'chmod u+s /data/software/calculate-umask.rpm', and two 'll /data/software/ | grep cal' commands. The outputs show the file permissions changing from '-rwsr-xr-x' to '-rwSr--r--'.

```
root@buiduongthe:~  
[root@buiduongthe ~]# ll /usr/bin/passwd  
-rwsr-xr-x. 1 root root 27856 Apr  1 2020 /usr/bin/passwd  
[root@buiduongthe ~]# touch /data/software/calculate-umask.rpm  
[root@buiduongthe ~]# chmod u+s /data/software/calculate-umask.rpm  
[root@buiduongthe ~]# ll /data/software/ | grep cal  
-rwSr--r--. 1 root root 0 Oct  9 16:11 calculate-umask.rpm  
[root@buiduongthe ~]# ll /data/software/ | grep cal  
-rwSr--r--. 1 root root 0 Oct  9 16:11 calculate-umask.rpm  
[root@buiduongthe ~]#
```

11. SGID

SGID hoặc Set GID, Group ID: Khi thiết lập SGID cho một thư mục thì tập tin và thư mục mới được tạo ra trong thư mục đó sẽ được kế thừa nhóm của thư mục đó.

A terminal window titled 'kd2@buiduongthe:/data/kinhdoanh' showing a series of commands and their outputs. The user sets permissions to 2777 on the directory, lists files, switches to user 'kd2', creates a file and a subdirectory, and then lists files again to show that the new files inherit the 'kinhdoanh' group.

```
kd2@buiduongthe:/data/kinhdoanh
[root@buiduongthe ~]# chmod -R 2777 /data/kinhdoanh/
[root@buiduongthe ~]# ll -l /data/ | grep kinhdoanh
drwxrwsrwx. 2 kd1  kinhdoanh 69 Oct  9 16:30 kinhdoanh
[root@buiduongthe ~]# su kd2
[kd2@buiduongthe root]$ cd /data/kinhdoanh/
[kd2@buiduongthe kinhdoanh]$ touch kd2_tailieu1.txt
[kd2@buiduongthe kinhdoanh]$ mkdir kd2_tailieu
[kd2@buiduongthe kinhdoanh]$ ll -l | grep kd2
-rwxrwsrwx. 1 root root    0 Oct  9 09:42 dulieukd2.txt
drwxrwsr-x. 2 kd2  kinhdoanh 6 Oct  9 16:32 kd2_tailieu
-rw-rw-r--. 1 kd2  kinhdoanh 0 Oct  9 16:31 kd2_tailieu1.txt
[kd2@buiduongthe kinhdoanh]$
```

11. SGID

chmod -R 2777 /data/kinhdoanh

Hoặc

chmod g+s /data/kinhdoanh

ll -l /data/ | **grep** kinhdoanh

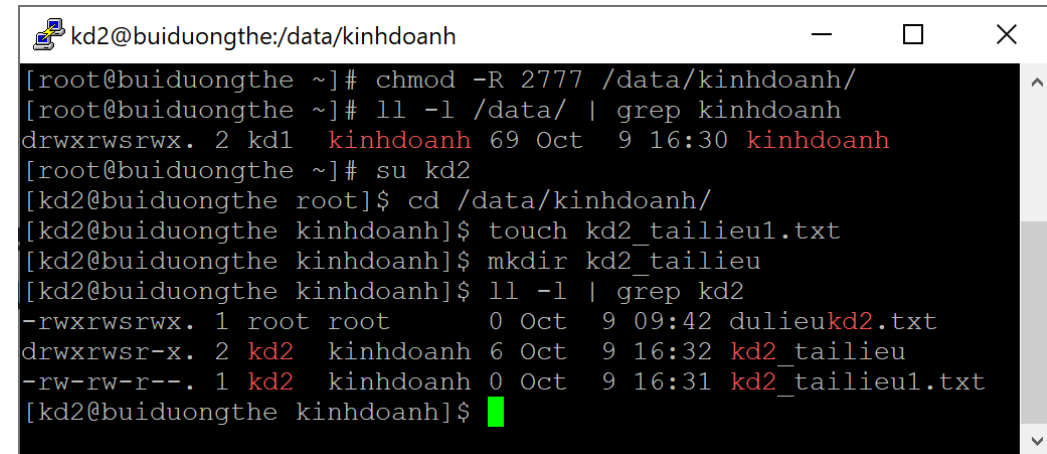
su kd2

\$ **cd** /data/kinhdoanh

\$ **touch** kd2_tailieu1.txt

\$ **mkdir** kd2_tailieu

\$ **ll -l** | **grep** kd2



```
kd2@buiduongthe:/data/kinhdoanh
[root@buiduongthe ~]# chmod -R 2777 /data/kinhdoanh/
[root@buiduongthe ~]# ll -l /data/ | grep kinhdoanh
drwxrwsrwx. 2 kd1 kinhdoanh 69 Oct  9 16:30 kinhdoanh
[root@buiduongthe ~]# su kd2
[kd2@buiduongthe root]$ cd /data/kinhdoanh/
[kd2@buiduongthe kinhdoanh]$ touch kd2_tailieu1.txt
[kd2@buiduongthe kinhdoanh]$ mkdir kd2_tailieu
[kd2@buiduongthe kinhdoanh]$ ll -l | grep kd2
-rwxrwsrwx. 1 root root    0 Oct  9 09:42 dulieukd2.txt
drwxrwsr-x. 2 kd2  kinhdoanh 6 Oct  9 16:32 kd2_tailieu
-rw-rw-r--. 1 kd2  kinhdoanh 0 Oct  9 16:31 kd2_tailieu1.txt
[kd2@buiduongthe kinhdoanh]$
```

12. Sticky Bit

Người dùng chỉ có thể xóa những tập tin mà chính họ tạo ra trong thư mục được thiết lập **Sticky bit**.

```
# chmod -R +t /data/ketoan
```

```
# chmod -R +t /data/kinhdoanh
```

```
# chmod -R +t /data/nhansu
```

Hoặc

```
# chmod -R 1775 /data/ketoan
```

```
# chmod -R 1775 /data/kinhdoanh
```

```
# chmod -R 1775 /data/nhansu
```

```
root@buiduongthe:~  
[root@buiduongthe ~]# chmod -R +t /data/ketoan  
[root@buiduongthe ~]# chmod -R +t /data/kinhdoanh/  
[root@buiduongthe ~]# chmod -R +t /data/nhansu/  
[root@buiduongthe ~]# ll -l /data/  
total 0  
drwxr-xr-t. 2 nv1 users 68 Oct 9 09:43 dulieu  
-rw-r--r--. 1 root root 0 Oct 9 09:47 HuongDan.txt  
drwxrwx--T. 2 kt1 ketoan 69 Oct 9 09:40 ketoan  
drwxrwsr-t. 3 kd1 kinhdoanh 112 Oct 9 16:32 kinhdoanh  
drwxrwxr-t. 2 ns1 nhansu 69 Oct 9 16:54 nhansu  
drwxr-xr-x. 2 sv1 student 69 Oct 9 09:42 sinhvien  
drwxr-xr-x. 2 root users 83 Oct 9 16:11 software  
drwxr-xr-t. 2 root root 6 Oct 9 15:37 umask  
drwxrwx---. 2 root root 6 Oct 9 15:41 umask_change  
-rw-rw----. 1 root root 0 Oct 9 15:41 umask_change.txt  
-rw-r--r--. 1 root root 0 Oct 9 15:37 umask.txt  
[root@buiduongthe ~]#
```

12. Sticky Bit

Tài khoản ns1, ns2, ns3 thuộc nhóm (group) nhân sự. Có quyền tạo thư mục và tập tin trong thư mục /data/nhansu

Đăng nhập tài khoản ns1

\$ **touch** /data/nhansu/ns1_vanban1.txt

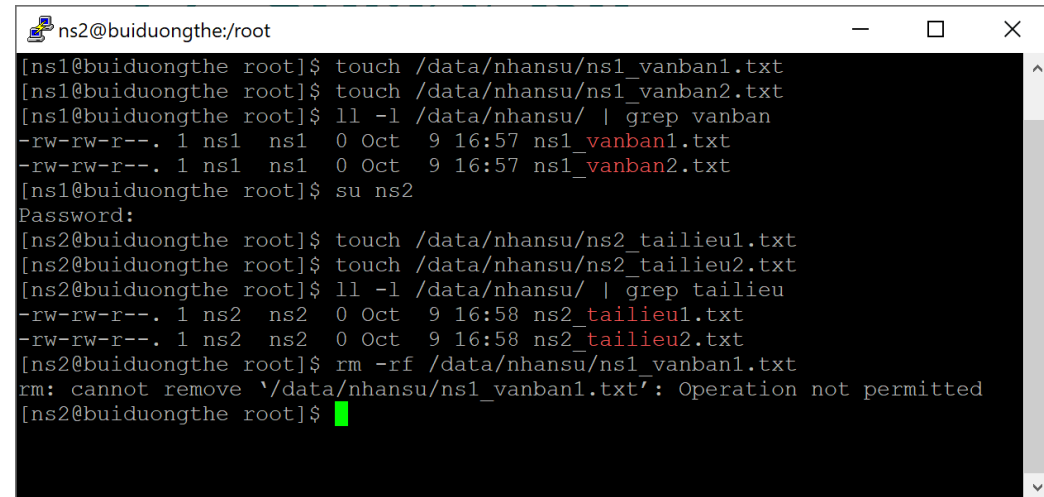
\$ **touch** /data/nhansu/ns1_vanban2.txt

Đăng nhập tài khoản ns2

\$ **touch** /data/nhansu/ns2_tailieu1.txt

\$ **touch** /data/nhansu/ns2_tailieu1.txt

\$ **rm -rf** /data/nhansu/ns1_vanban1.txt



```
ns2@buiduongthe:/root
[ns1@buiduongthe root]$ touch /data/nhansu/ns1_vanban1.txt
[ns1@buiduongthe root]$ touch /data/nhansu/ns1_vanban2.txt
[ns1@buiduongthe root]$ ll -l /data/nhansu/ | grep vanban
-rw-rw-r--. 1 ns1  ns1  0 Oct  9 16:57 ns1_vanban1.txt
-rw-rw-r--. 1 ns1  ns1  0 Oct  9 16:57 ns1_vanban2.txt
[ns1@buiduongthe root]$ su ns2
Password:
[ns2@buiduongthe root]$ touch /data/nhansu/ns2_tailieu1.txt
[ns2@buiduongthe root]$ touch /data/nhansu/ns2_tailieu2.txt
[ns2@buiduongthe root]$ ll -l /data/nhansu/ | grep tailieu
-rw-rw-r--. 1 ns2  ns2  0 Oct  9 16:58 ns2_tailieu1.txt
-rw-rw-r--. 1 ns2  ns2  0 Oct  9 16:58 ns2_tailieu2.txt
[ns2@buiduongthe root]$ rm -rf /data/nhansu/ns1_vanban1.txt
rm: cannot remove '/data/nhansu/ns1_vanban1.txt': Operation not permitted
[ns2@buiduongthe root]$
```

13. Access Control List

Cho phép quản lý phân quyền chi tiết

Cho phép áp dụng tập hợp các quyền cụ thể cho tập tin hoặc thư mục mà không nhất thiết phải thay đổi quyền sở hữu.

Cho phép bổ sung quyền truy cập cho tài khoản hoặc nhóm khác

getfacl --help

setfacl --help

13. Access Control List

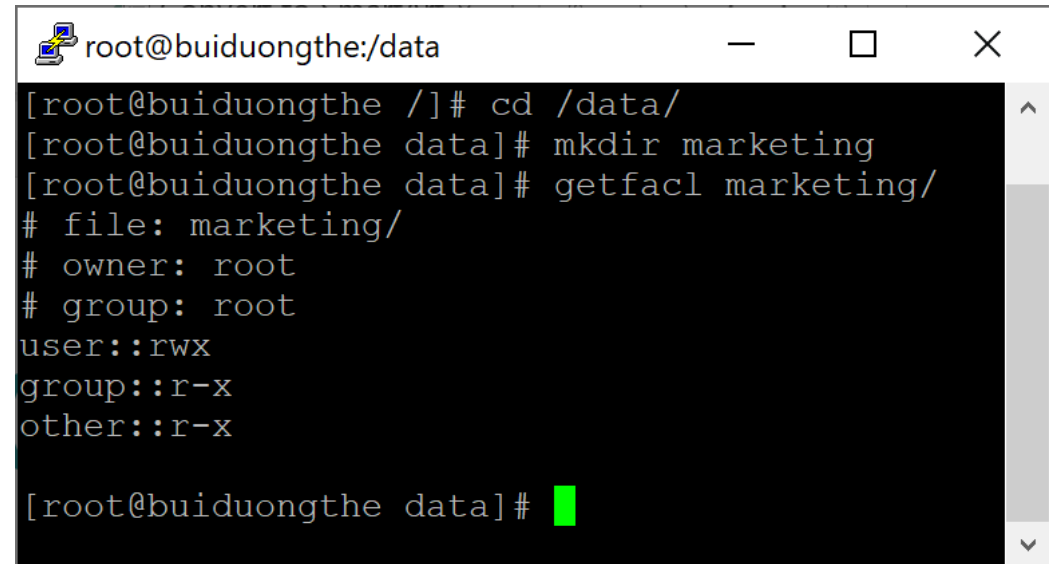
Xem thông tin ACL

cd /data

mkdir marketing

getfacl marketing

Access ACL: áp dụng cho cả tập tin và thư mục

A terminal window titled 'root@buiduongthe:/data' with standard window controls. The terminal shows a sequence of commands: 'cd /data/', 'mkdir marketing', and 'getfacl marketing/'. The output of 'getfacl' lists permissions for the 'marketing/' directory: owner (root), group (root), user permissions (rwx), group permissions (r-x), and other permissions (r-x). The prompt is currently at '[root@buiduongthe data]#'.

```
root@buiduongthe:/data
[root@buiduongthe /]# cd /data/
[root@buiduongthe data]# mkdir marketing
[root@buiduongthe data]# getfacl marketing/
# file: marketing/
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

[root@buiduongthe data]#
```

13. Access Control List

Thiết lập Default ACL

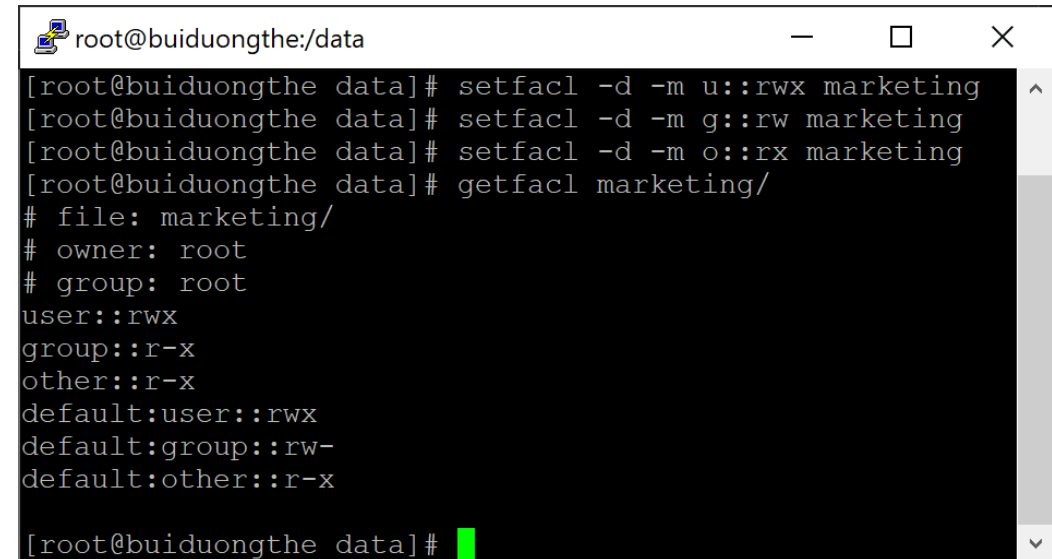
```
# setfacl -d -m u::rwx marketing
```

```
# setfacl -d -m g::rw marketing
```

```
# setfacl -d -m o::rx marketing
```

```
# getfacl marketing
```

Default ACL: Chỉ áp dụng cho thư mục, xác định quyền thừa kế từ thư mục cha khi được tạo



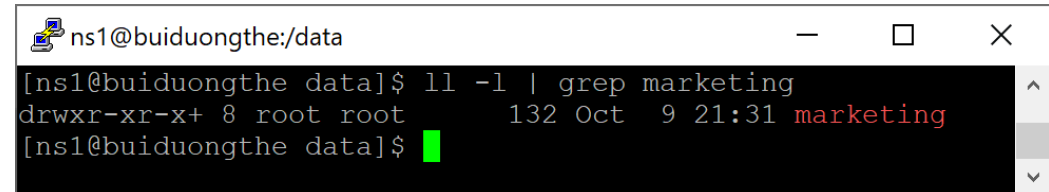
```
root@buiduongthe:/data
[root@buiduongthe data]# setfacl -d -m u::rwx marketing
[root@buiduongthe data]# setfacl -d -m g::rw marketing
[root@buiduongthe data]# setfacl -d -m o::rx marketing
[root@buiduongthe data]# getfacl marketing/
# file: marketing/
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
default:user::rwx
default:group::rw-
default:other::r-x
[root@buiduongthe data]#
```

13. Access Control List

Thiết lập Default ACL

\$ **ll -l | grep** marketing

Cột đầu tiên chứa một dấu +, đây là ký tự đại diện cho một extended ACL



```
ns1@buiduongthe:/data
[ns1@buiduongthe data]$ ll -l | grep marketing
drwxr-xr-x+ 8 root root      132 Oct  9 21:31 marketing
[ns1@buiduongthe data]$
```

13. Access Control List

Thiết lập Default ACL

cd marketing

mkdir default_acl_1

mkdir default_acl_2

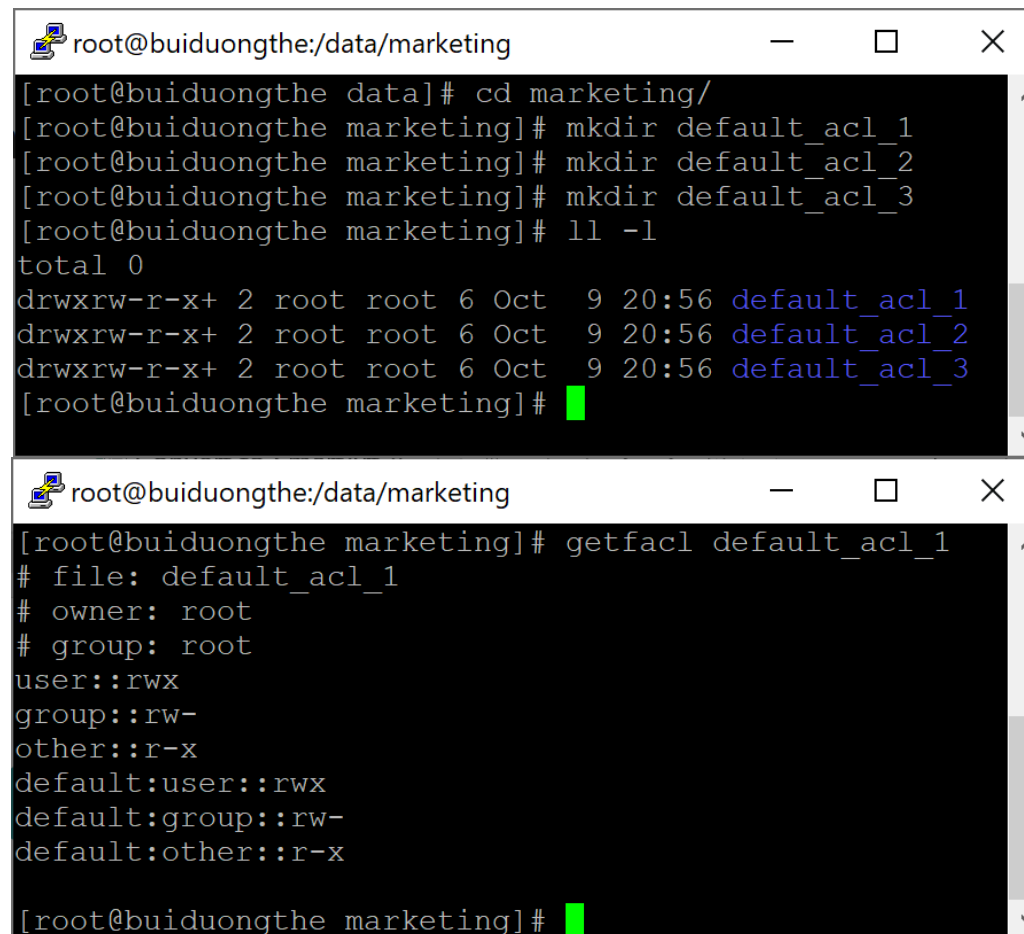
mkdir default_acl_3

ll -l

getfacl default_acl_1

su ns1

\$ **touch** default_acl_1/ns1_tailieu.txt



```
root@buiduongthe:/data/marketing
[root@buiduongthe data]# cd marketing/
[root@buiduongthe marketing]# mkdir default_acl_1
[root@buiduongthe marketing]# mkdir default_acl_2
[root@buiduongthe marketing]# mkdir default_acl_3
[root@buiduongthe marketing]# ll -l
total 0
drwxrw-r-x+ 2 root root 6 Oct  9 20:56 default_acl_1
drwxrw-r-x+ 2 root root 6 Oct  9 20:56 default_acl_2
drwxrw-r-x+ 2 root root 6 Oct  9 20:56 default_acl_3
[root@buiduongthe marketing]#

root@buiduongthe:/data/marketing
[root@buiduongthe marketing]# getfacl default_acl_1
# file: default_acl_1
# owner: root
# group: root
user::rw-
group::rw-
other::r-x
default:user::rw-
default:group::rw-
default:other::r-x
[root@buiduongthe marketing]#
```

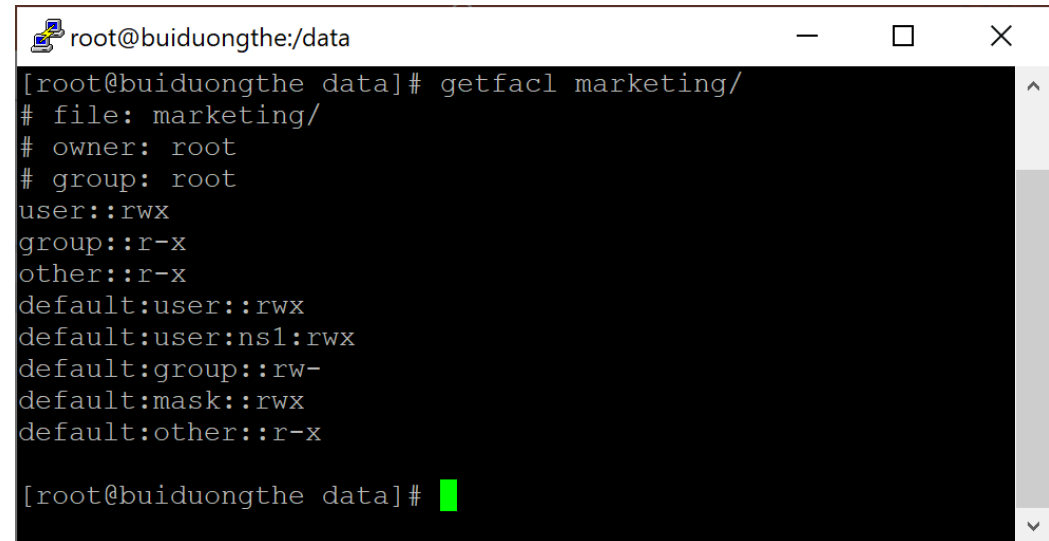
13. Access Control List

Thiết lập Default ACL

cd /data

setfacl -d -m u:ns1:rwX marketing

getfacl marketing



```
root@buiduongthe:/data
[root@buiduongthe data]# getfacl marketing/
# file: marketing/
# owner: root
# group: root
user::rwX
group::r-x
other::r-x
default:user::rwX
default:user:ns1:rwX
default:group::rw-
default:mask::rwX
default:other::r-x

[root@buiduongthe data]#
```

13. Access Control List

Thiết lập Default ACL

mkdir default_acl_4

mkdir default_acl_5

mkdir default_acl_6

ll -l

Thấy quyền đã được thay đổi, đăng nhập tài khoản **ns1** để tạo tập tin hoặc thư mục trên các thư mục **default_acl_***

\$ **touch** default_acl_1/ns1_tailieu.txt

\$ **touch** default_acl_4/ns1_tailieu.txt

```
root@buiduongthe:/data/marketing
[root@buiduongthe data]# setfacl -d -m u:ns1:rwX marketing
[root@buiduongthe data]# cd marketing/
[root@buiduongthe marketing]# mkdir default_acl_4
[root@buiduongthe marketing]# mkdir default_acl_5
[root@buiduongthe marketing]# mkdir default_acl_6
[root@buiduongthe marketing]# ll -l
total 0
drwxrw-r-x+ 2 root root 6 Oct  9 20:56 default_acl_1
drwxrw-r-x+ 2 root root 6 Oct  9 20:56 default_acl_2
drwxrw-r-x+ 2 root root 6 Oct  9 20:56 default_acl_3
drwxrwxr-x+ 2 root root 6 Oct  9 21:31 default_acl_4
drwxrwxr-x+ 2 root root 6 Oct  9 21:31 default_acl_5
drwxrwxr-x+ 2 root root 6 Oct  9 21:31 default_acl_6
[root@buiduongthe marketing]#
```

```
ns1@buiduongthe:/data/marketing
[ns1@buiduongthe marketing]$ touch default_acl_1/ns1_tailieu.txt
touch: cannot touch 'default_acl_1/ns1_tailieu.txt': Permission denied
[ns1@buiduongthe marketing]$ touch default_acl_4/ns1_tailieu.txt
[ns1@buiduongthe marketing]$
```

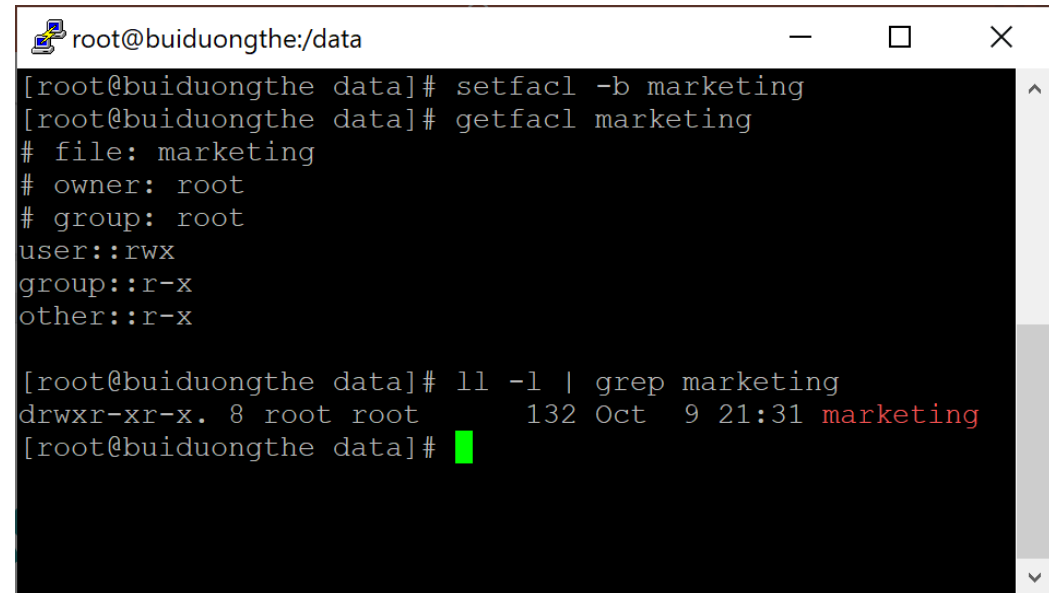
13. Access Control List

Xóa ACL

setfacl -b marketing

getfacl marketing

ll -l | group marketing

A terminal window titled 'root@buiduongthe:/data' with standard window controls. It displays a series of commands and their outputs. The commands are: 'setfacl -b marketing', 'getfacl marketing', and 'll -l | grep marketing'. The outputs show the file's permissions, owner, group, and the resulting ACL for the 'marketing' group.

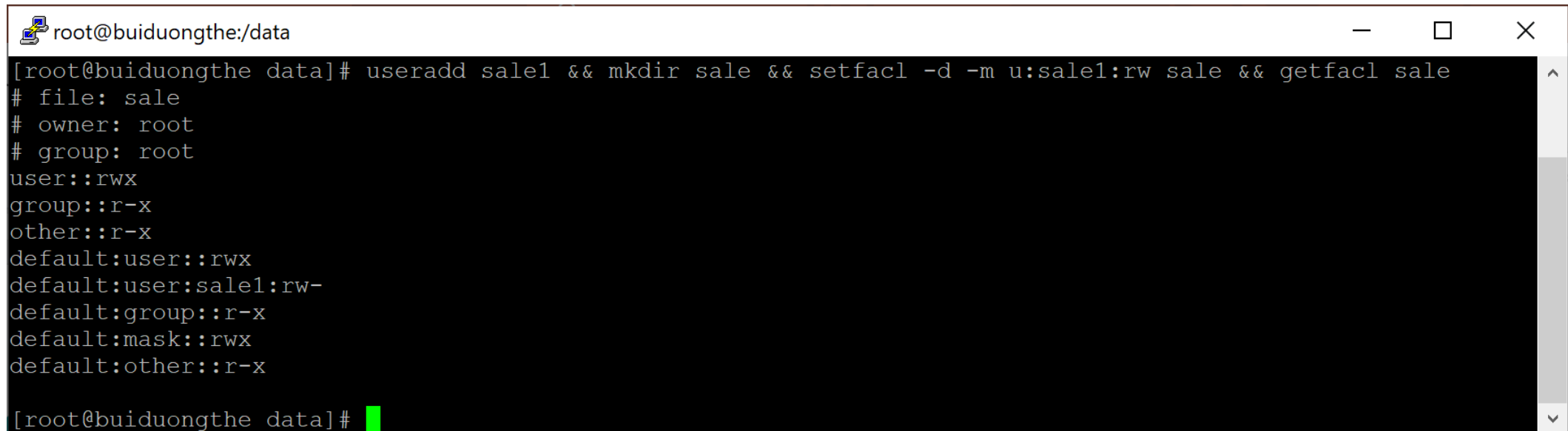
```
root@buiduongthe:/data
[root@buiduongthe data]# setfacl -b marketing
[root@buiduongthe data]# getfacl marketing
# file: marketing
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

[root@buiduongthe data]# ll -l | grep marketing
drwxr-xr-x. 8 root root      132 Oct  9 21:31 marketing
[root@buiduongthe data]#
```

13. Access Control List

Hướng dẫn thực thi đồng thời các lệnh

useradd sale1 && **mkdir** sale && **setfacl** -d -m u:sale1:rw sale && **getfacl** sale



```
root@buiduongthe:/data
[root@buiduongthe data]# useradd sale1 && mkdir sale && setfacl -d -m u:sale1:rw sale && getfacl sale
# file: sale
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
default:user::rwx
default:user:sale1:rw-
default:group::r-x
default:mask::rwx
default:other::r-x
[root@buiduongthe data]#
```


Bài tập

- Thực hiện theo slide hướng dẫn
- Xây dựng cấu trúc lưu trữ dữ liệu công ty và phân quyền như sau:
 - Nhân viên của phòng ban nào chỉ có quyền truy cập vào thư mục của phòng ban đó.
 - Nhân viên chỉ được xóa những tập tin/thư mục do chính nhân viên đó tạo ra.
 - Trưởng phòng được xóa dữ liệu của phòng đó.
 - Giám đốc có thể truy cập, thêm, xóa, sửa vào tất cả các dữ liệu của các phòng ban
 - Chụp hình kết quả cây thư mục có phân quyền
- Ôn tập và thực các lệnh đã học

Tài liệu

TT	Tên tác giả	Năm XB	Tên sách, giáo trình, tên bài báo, văn bản	NXB, tên tạp chí/ nơi ban hành VB
1	Dennis Matotek James Turnbull Peter Lieverdink	2017	Pro Linux System Administration Trang (147-180)	Apress

THẢO LUẬN